CHAPTER 7

Protecting Election Infrastructure: A View from the Federal Level

Matthew Masterson

Abstract Securing elections and democracy in the United States requires adaptation and innovation in the field. The adoption and implementation of new strategies and procedures is not without risk. Ensuring the system is solvent and secure, once viewed solely under the purview of states and local governments, the security of elections in the United States has evolved to be an issue of concern and investment at all levels of government. The increased involvement of federal agencies in the administration of elections in the United States has created new opportunities for the development of intergovernmental relationships and resources. Discussed in this case is the role of the Department of Homeland Security in election administration, as experienced by one election administration expert.

Keywords Cybersecurity • Vendors • Security • Information • Intergovernmental relationships

M. Masterson (✉)
United States Department of Homeland Security,
Washington, DC, USA
e-mail: matthew.masterson@hq.dhs.gov

M. Brown et al. (eds.), *The Future of Election Administration*, Elections, Voting, Technology, https://doi.org/10.1007/978-3-030-18541-1_7

I began my career in elections as Special Assistant/Counsel to Chairman Paul DeGregorio, working with the US Election Assistance Commission (EAC) updating the Voluntary Voting System Guidelines (VVSG) through the Voting System Testing and Certification Program, and working with the laboratory accreditation program. From there I moved to the Office of the Secretary of State for Ohio, and then from 2015 to 2018 I served as a Commissioner for the EAC including serving as its Chairman in 2017. Today I work as a senior advisor for the Department of Homeland Security, leading their election security work. The unifying theme in my career in US elections is equipment and technology.

I tell people all the time the best part of my job is that I wake up in the morning and know the importance of my work. I don't lack motivation because I work with incredible people to maintain the integrity of our democracy. My inspiration goes beyond the "God Bless America" democracy space—my commitment is to be able to help people to identify and manage risk in the election process, to continue to modernize that process, and to improve services to voters. I believe that the single worst thing that could happen to US elections is for us to move away from improving services and modernization because we are afraid of risk. We need to assess and manage that risk in order to move forward. This is what my work in elections is about.

Today, election systems have been classified as critical infrastructure, and that has had a significant influence on my work. From my perspective, elections have always been a part of the critical infrastructure of the US because they are essential to maintaining American democracy. Being officially part of critical infrastructure since 2016 means that we, the Department of Homeland Security, can prioritize the efforts of the federal government to support the work of state and local officials, all with the overarching goal of providing state and local election officials and their private partners the tools that they need to identify and mitigate risk.

Improvements in Election Security, 2016–2018

Securing elections is not new to election officials. They have long worked to ensure the security and integrity of the process. However, following the 2016 election and the known attempts by sophisticated actors to interfere with our elections, there was a paradigm shift. Improvements in cyber readiness began happening almost immediately after the designation of elections as critical infrastructure. Our work to date has focused around

information sharing, providing support and services, coordination across the federal government, and Election Day monitoring and sharing. Together these activities have significantly advanced our response capability across the nation.

First, we built information sharing capacity across the elections community to understand the general risk environment, specific threats, and how to mitigate these. We did this through the development of the Elections Infrastructure Information Sharing Analysis Center (EI-ISAC), created in February 2018. Between February and November 2018, we were able to provide all 50 states and over 1400 local jurisdictions with general information and specific technical indicators around election security and a path for reporting back to the EI-ISAC. This system gives states and localities an avenue to report information to us, which has resulted in the most significant improvement to date.

In 2018, state and local officials robustly shared this information, including technical information and potential threats from social media campaigns. For example, officials in the State of Vermont provided us technical indicators that occurred when targeting their system. We shared this information widely, and several states investigated this in their own systems and reported back that they saw this activity as well, and as a result, we were able to release an alert nationally. This process took about a week, and was very successful and is exactly how this cycle is supposed to work. As good as the information from the intelligence community is, the best information came from election officials on the ground.

Another example comes from the deployment of Albert sensors. These sensors are part of an intrusion detection system collecting information about traffic targeting election infrastructure and alerts related to known, malicious actors. Prior to 2016 there were only a handful of state election infrastructures covered by Albert systems, and in these cases they were indirectly covered through other state systems that were connected to elections, not through the election infrastructure specifically. By Election Day 2018, 46 states and 90 localities had Albert sensors covering their specific election infrastructures. These sensors gave us a good understanding of the baseline of activity that was targeting election infrastructure; this will help us moving into 2020 to determine when things are out of the range of normal.

Second, we also provided direct support and services to states and localities. As part of the critical infrastructure designation, election officials and their private sector partners are prioritized to receive Department of

Homeland Security (DHS) services. These include scanning for known vulnerabilities, on-site penetration testing of systems, phishing campaign assessments over 12 weeks with increasing complexity, cyber resilience reviews of cyber architecture, and resilience reviews with advice on how to build more resilient physical security of election offices and polling places. All of these services are free and intended to identify risk and empower officials and vendors to mitigate those risks. A majority of states and several hundred jurisdictions have taken advantage of at least one of these services.

Third, we enhanced coordination across the federal government. In 2016, we learned that federal agencies were not prepared to work together around cyber threats to elections. DHS took the lead to coordinate agencies and organizations at the national level. This included the Federal Bureau of Investigation (FBI), the Department of Defense (DOD), the National Security Agency (NSA), Cybercom, the Office of the Director of National Intelligence (ODNI), the National Institute of Standards and Technology (NIST), and the EAC. A significant improvement comes out of this—our ability to take intelligence, put that in a format that can be shared, and push that information out nationally through the EI-ISAC, the EAC, the National Association of Secretaries of State (NASS), and the National Association of State Election Directors (NASED). These groups are committed to pushing that information to local offices for information sharing. We also offered security clearances to state chief election officials (CEOs) and two of their designees in each state to enhance our ability to share specific threat and general intelligence to help election offices prepare and respond. Throughout 2018, we utilized these clearances to provide classified briefings to state election officials regarding the threat environment around elections and steps they can take to manage risks and share information with the community. To date, most of this information has actually involved election disinformation rather than targeting of election infrastructure. Having the ability to push this information down to the election community is an incredible resource that was not there before the designation of elections as critical infrastructure.

Finally, on Election Day for major elections, this work is also about communication and coordination. As an example, on Election Day 2018, we stood up an operation center in Arlington, Virginia, with representatives from DHS, our other federal partners, NASS, NASED, the Republican National Committee (RNC), the Democratic National Committee (DNC), voter protection hotline, and private sector vendors, all to share and respond to information. As part of this, we established a cyber-situational

awareness room with over 600 active state and local election office partners across the country who shared information about cyber activity. We investigated and shared information with election officials around the country as necessary through this mechanism. This also included contact with social media companies throughout the day. As another example, in Ohio a voter released a video through social media of a piece of election equipment presumably flipping votes. The officials from that county (Franklin County) were able to quickly identify that specific piece of equipment, diagnose the problem (paper jamming), and contact the state with information about the problem and the fix of it. Then, we were able to provide feedback through social media and the general media to shut down misinformation and educate the public about what was actually happening. This is a great example of our information sharing capabilities.

Improvements in Election Security Moving Forward

Coming out of the 2018 midterm elections, there are a number of areas that can be improved. Nationally, we did a good job developing our information sharing system, but we still need to work on engaging people at the local level, especially local election officials in the mid- to small-sized jurisdictions. We need to double down on what we refer to as our "Last Mile" project to reach these offices. The Last Mile will allow states to push information to counties and other election jurisdictions about risks to their specific election systems, possible mitigations, and state specific checklists to improve their cyber hygiene. We need to improve and educate those mid- to small-sized counties, townships, and cities so we can reach everyone. We still have over 7000 jurisdictions that we need to find a way to partner with and support.

We also need to work on "maturing" our discussions about risk. It is challenging to have open and mature discussions about risk because we are afraid of negatively impacting the public's confidence in the process. But we need to have open, honest, and transparent conversations with all of the relevant stakeholders, including county commissioners, state legislatures, and other funding and policy bodies. The message we need to distribute is "Here are all of the great things we were able to do given current funding levels, but if we had more resources and regular investment, here is what we could do." We need to educate policy makers at all levels about what it means to meaningfully invest—in training, technology, upgrades, and information technology (IT) personnel. Some states are doing this.

For example, Washington, Illinois, and Florida are deploying cyber navigators from state offices to counties that have little to no IT support—this is a tangible risk management technique that states can implement that is not just buying new equipment.

Finally, we need to both continue and broaden our engagement with private sector partners. Many counties are reliant on their vendors. Consequently, we must build strong, trusting relationships with all of the vendors involved in elections across election sub-systems. We must and will invest time and resources to build trust with this group of election stakeholders.